

Microsoft365対応パックの内容について

Microsoft 365対応バック 検知リスト



SharePoint



OneDrive
for Business

ファイルアクセス

- ・共有リンク（匿名リンク、セキュリティで保護されたリンク）によるデータ共有
- ・ファイルアクセス（移動/コピー/削除/復元）
- ・ファイルのダウンロード/アップロード監視
- ・ファイル/フォルダ/サイトの共有監視
- ・業務時間外のファイルアクセス
- ・職場のグローバルIP以外からのファイルアクセス
- ・組織外ユーザーによるファイルアクセス/ダウンロード
- ・公開フォルダへのファイルコピー



Exchange

メール

- ・メールボックスへのサインイン
- ・代理送信機能を使ったメール送付
- ・大量メール送信の検出
- ・検疫/スパムメールの受信者集計
- ・大容量ファイルのメール送信検知
- ・DLP（データ漏洩防止）検出
- ・メール送信失敗
- ・転送設定の変更検知



Azure



AD認証/管理者操作

- ・グループへのメンバー追加、グループからのメンバー削除
- ・グループの作成/削除
- ・ユーザーアカウントの作成/削除
- ・パスワードの再設定（リセット）
- ・組織外ユーザーの作成/削除、グループへの追加
- ・職場のグローバルIP以外からのログイン
- ・大量ログイン失敗
- ・業務時間外のログイン
- ・その他のAD管理イベント



TEAMS



チャット

- ・TEAMSへのサインイン
- ・チームの作成/変更/削除
- ・チャネルの追加/変更/削除

テンプレートの利用方法（取り込み編）

◆テンプレートのインポート手順

The screenshot shows the ALog management interface. The top navigation bar includes 'ホーム' (Home), '検索' (Search), 'レポート / アラート' (Report / Alert), and '管理' (Management). The '管理' tab is highlighted with a red box and a callout bubble labeled '①管理タブをクリック' (Click the Management tab). The left sidebar contains various settings, with '設定のインポート / エクスポート' (Import / Export Settings) highlighted with a red box and a callout bubble labeled '②「設定のインポート/エクスポート」タブをクリック' (Click the 'Import/Export Settings' tab). The main content area shows the 'ステータス' (Status) section with a table of tasks.

サーバ	タスクの種類	タスクの状態	次の実行日時	前回の実行日時	前回の実行結果	アクセスログ...	
S-2019SK	ログ変換	準備完了	2019/10/16 16:40:00	2019/10/16 16:30:00	正常終了	0	タスクの操作▼
S-2019SK	インポート	準備完了	-	2019/10/16 16:30:00	正常終了		タスクの操作▼
S-2019SK	レポート	準備完了	2019/10/17 2:00:00	2019/10/16 16:33:00	正常終了		タスクの操作▼
S-2019SK	AD情報取得	準備完了	2019/10/17 1:00:00	2019/10/16 16:33:00	正常終了	2545	タスクの操作▼
S-2019SK	メンテナンス	準備完了	2019/10/17 3:00:00	-			タスクの操作▼
S-2019SK	リスク学習	準備完了	2019/11/01 0:00:00	-			タスクの操作▼

テンプレートの利用方法について (取り込み編)

設定のインポート / エクスポート

設定のインポート/エクスポートを行います。

④ エクスポート

⑤ レポート / アラート

レポート名

- ☐ サーバアクセスランキング
- ☐ ファイルアクセスランキング
- ☐ ファイルの読込
- ☐ ログオン失敗
- ☐ 時間別アクセス
- ☐ 土日のアクセス
- ☐ 夜間のアクセス

⑥ 休日・祝日設定

名称

- ☐ 年末の休業日
- ☐ 年始の休業日

⑦ EVAテンプレート

テンプレート名

- ☐ NetApp (NFSv4)
- ☐ Webサーバ((IIS7)
- ☐ Webサーバ((IIS8)

⑧ エクスポート

⑨ インポート

⑩ インポート

③参照ボタンをクリック

名前	状態	更新日時	種類
03_ユーザーアカウントの作成、削除	⊙	2022/08/08 18:34	ファイル フォルダ
04_パブリックの作成、削除 (H・M)	⊙	2022/08/08 18:34	ファイル フォルダ
05_...	⊙	2022/08/08 18:34	ファイル フォルダ
06_...	⊙	2022/08/08 18:34	ファイル フォルダ
07_...	⊙	2022/08/08 18:34	ファイル フォルダ
08_...	⊙	2022/08/08 18:34	ファイル フォルダ
09_組織外ユーザの作成・前...	⊙	2022/08/08 18:34	ファイル フォルダ
10_ファイルアクセス(移動、コピー、削除)	⊙	2022/08/08 18:34	ファイル フォルダ
11_ファイルアップロード、ダウンロード	⊙	2022/08/08 18:34	ファイル フォルダ
12_ファイル、フォルダ、サイトの共有監視	⊙	2022/08/08 18:34	ファイル フォルダ
13_業務時間外のファイルアクセス	⊙	2022/08/08 18:34	ファイル フォルダ
14_名前	状態	更新日時	種類
15_	⊙	2022/04/13 14:49	XML ドキュメント
16_	⊙	2022/04/13 14:49	XML ドキュメント
17_...	⊙	2022/08/08 18:34	ファイル フォルダ
18_メールボックスへのサインイン	⊙	2022/08/08 18:34	ファイル フォルダ

④取り込みたいレポート定義を選択
(フォルダ毎の指定が可能です)

setting-2020-1009-085906990_output

⑪ インポート

C:\fakepath\setting-2020-1009-085906990_output.xml

参照

☒ レポートテンプレート: 1 件

⑫ インポート

⑤インポートボタンをクリック

テンプレートの利用方法について（取り込み編）

◆ 注意点

- 全ての**レポートテンプレート**を取り込みたい場合、以下フォルダ内のファイル（setting-2021-xxxxxxx.xml）をインポートして下さい。

22_検疫、スパムメールの受信者集計	✓	2022/08/08 18:34
23_大容量ファイルのメール送信検知	✓	2022/08/08 18:34
24_大量メール送信の検出	✓	2022/08/08 18:34
25_転送設定の変更検知	✓	2022/08/08 18:34
26_Teamsへのサインイン	✓	2022/08/08 18:34
27_チームの作成、変更、削除	✓	2022/08/08 18:34
28_チャンネルの追加、変更、削除	✓	2022/08/08 18:34
一括インポート	✓	2022/08/08 18:34
レポート設定参考資料_MS365編	✓	2022/08/09 9:04
自動化パックの内容及び利用方法について（Microsoft365...	🔄	2022/08/09 10:10

名前	状態	更新日時
setting-2021-1224-133012317_output	✓	2022/04/13 15:04

※個別のレポートテンプレートのみを取り込みたい場合、各フォルダに格納されているxmlファイルを取り込んで下さい。

テンプレートの利用方法について（取り込み編）

◆ 注意点②

- ・ Microsoft365のログを初めて取得する場合、別途EVAプラグインをインストールする必要があります。
取り込み用テンプレート（プラグイン）、については担当営業もしくは資料末尾記載の網屋窓口へお問い合わせください。
各フォルダ内に格納された「install_guide」を参考に次ページの対象登録を実施頂く必要があります。



対象機器の追加（※Microsoft365のログを未取得のお客様）

◆Microsoft365のログを初めて取得する場合、対象機器の追加が必要となります。

The screenshot shows the ALog management interface. The top navigation bar is green and contains the ALog logo, home icon, search icon, report/alert icon, risk scoring icon, WorkTime icon, and a management icon (highlighted with a red box). The left sidebar contains a list of menu items: Status, Status, Statistics, System Log, User Operation Log, System Log, and Settings. The 'Settings' item is highlighted with a red box. The main content area is titled '対象サーバ' (Target Servers) and contains instructions: 'ログの収集対象となるサーバの設定を行ないます。' and 'サーバの追加/削除やログの収集タスクの設定を行ないます。'. Below the instructions is a table with columns: 選択 (Select), サーバ (Server), サーバ種別 (Server Type), 収集タイプ (Collection Type), バージョン (Version), アカウント (Account), 収集タスク (Collection Task), and ログ種別 (Log Type). The table lists two servers: AMIYADemo (Windows, Agentless, 8.1.5, Administrator, Ineffective, File Access Log, Log On Log) and Blue Coat ProxySG (EVA, Agentless, 8.1.5, -, Ineffective, -). Above the table are buttons: '+ 追加' (Add), '削除' (Delete), 'エージェントのアップデート' (Update Agent), and '収集タスクの設定' (Set Collection Task). The '+ 追加' button is highlighted with a red box.

■	サーバ	サーバ種別	収集タイプ	バージョン	アカウント	収集タスク	ログ種別
<input type="checkbox"/>	AMIYADemo	Windows	エージェントレス方式	8.1.5	Administrator	●無効	ファイルアクセスログ, ログオンログ
<input type="checkbox"/>	Blue Coat ProxySG	EVA	エージェントレス方式	8.1.5	-	●無効	-

「管理」タブ - 「対象サーバ」 - 「追加」をクリック頂くと、「対象サーバ追加ウィザード」が開きますので、対象機器の登録をお願いします。詳細はユーザガイドをご参照下さい。
※Microsoft365のログを取得する場合、「ALog EVA」のライセンスが必要です。

テンプレートの利用方法（確認編）

テンプレートの利用方法について（確認編）

① レポート / アラートタブをクリック

ホーム 検索 レポート / アラート

フィルター 確認済みにする 操作

新規作成

■ お気...	レポート名	概要説明	未確認ア...	最終更新日時	状態	有効な機能	PDF...	CSV...	メ...	編集
<input type="checkbox"/>	★ イベントログ削除		🚨 未確...	2022/08/08 17:33	✓	📄 🚨 🛡				

② 新規作成をクリック

新規作成 - テンプレート選択

標準テンプレート

基本監査パック

サイバー攻撃自動検知パック

Microsoft 365 パック

ライセンスを登録してからレポートを設定してください

🔑 Microsoft 365 パック

MS365 (Azure Active Directory) : グループの作成、削除	グループの作成、削除を監視します。
MS365 (Azure Active Directory) : グループへのメンバー追加、グループからのメンバー削除	グループへのメンバー追加、グループからのメンバー削除を監視します。
MS365 (Azure Active Directory) : その他の AD 管理イベント	その他の AD 管理イベントを監視します。以下Operation以外のAD管理イベントを監視します。 ・グループの作成、削除 ・グループの更新 ・グループへのメンバー追加、削除 ・グループ所有者の追加、削除 ・ユーザの更新 ・ユーザ追加、削除
MS365 (Azure Active Directory) : パスワードの再設定 (リセット)	Microsoft365 (Azure Active Directory) に対するパスワードの再設定 (リセット) を定常的にモニタリングします。適切な申請に基づいたパスワードの再設定 (リセット) が否か、異常な回数の再設定 (リセット) ログが無いかを確認して下さい。
MS365 (Azure Active Directory) : ユーザーアカウントの作成/削除	Microsoft365 (Azure Active Directory) のユーザーアカウントの作成/削除を監視します。申請に基づいたアカウントの作成/削除が、不必要なアカウントの作成が行われていないか確認して下さい。

③ レポートがインポートされている事を確認

テンプレートの利用方法（作成編）

◆取り込んだレポートテンプレートをもとにお客様環境に合ったレポートを作成しましょう。 ※別ファイル「レポート設定参考資料」を参照下さい。

ALog ホーム 検索 レポート / アラート 管理

フィルター 確認済みにする 操作

新規作成 - テンプレート選択

お気に入り	
<input type="checkbox"/>	イベントログ削除

標準テンプレート

ライセンスを登録してからレポートを設定してください

基本監査パック

サイバー攻撃自動検知パック

[Microsoft 365 パック](#)

MS365 (Azure Active Directory) : グループの作成、削除

MS365 (Azure Active Directory) : グループへのメンバー追加、グループからのメンバー削除

MS365 (Azure Active Directory) : その他の AD 管理イベント

MS365 (Azure Active Directory) : パスワードの再設定 (リセット)

MS365 (Azure Active Directory) : 大量ログイン失敗

グループの作成、削除を監視します。

グループへのメンバー追加、グループからのメンバー削除を監視します。

その他の AD 管理イベントを監視します。以下Operation以外のAD管理イベントを監視します。・グループの作成、削除・グループの更新・グループへのメンバー追加、削除・グループ所有者の追加、削除・ユーザの更新・ユーザ追加、削除

Microsoft 365 (Azure Active Directory) : パスワードの再設定 (リセット) を定期的にモニタリングします。パスワードの変更 (リセット) が正常に完了したかどうか、異常な状態を検出します。

Microsoft 365 (Azure Active Directory) に対する大量のログイン失敗をモニタリングします。このレポートでは一人当たり1時間に5回以上のログイン失敗があった場合、アラート発報するように定義しています。 ※必要に応じてしきい値及び間隔を変更して下さい。

作成したいレポートをクリック

テンプレートの利用方法について（作成編）

新規作成 - MS365 (Azure Active Directory) : 大量ログイン失敗

状態 ☒ 有効 ☐ 無効

レポート名 MS365 (Azure Active Directory) : 大量ログイン失敗

概要説明 Microsoft365 (Azure Active Directory) に対する大量のログイン失敗をモニタリングします。

このレポートでは一人当たり1時間に5回以上のログイン失敗があった場合、アラート発報するように定義しています。

レポート名及び概要説明はお客様環境に応じてわかりやすいよう指定して下さい。

「制限しない」がONの場合、大量のアクセスログがヒットした際にパフォーマンスが低下する可能性があります。このレポートでは、フィルタ条件が厳しく、ヒットするアクセスログが限られているレポートでの利用を推奨します。

当レポートではOperation部分にMicrosoft365へのログイン失敗である「UserLoginFailed」を指定しています。

条件1

操作 選択なし ▼ 操作一覧

Operation [対象とする] UserLoginFailed [除外する]

複数指定する場合、改行区切りで入力します。

しきい値 ? + 5 - しきい値の間隔 1時間 ▼

当レポートではしきい値を「5」、しきい値の間隔を「1時間」としています。お客様環境に合わせて変更をお願いします。

テンプレートの利用方法について (作成編)

新規作成 - MS365 (Azure Active Directory) : 大量ログイン失敗

状態 ☒ 有効 ☐ 無効

機能 ☒ レポート ☒ アラート ☐ リスクスコアリング

レポート名 MS365 (Azure Active Directory) : 大量ログイン失敗

概要説明 Microsoft365 (Azure Active Directory) に対する大量のログイン失敗をモニタリングします。

このレポートでは一人当たり1時間に5回以上のログイン失敗があった場合、アラート発報するように定義しています。

出力件数 ☒ 制限しない

「制限しない」がONの場合、大量のアクセスログがヒットした際にパフォーマンスが悪化する可能性があります。フィルター条件が厳しく、ヒットするアクセスログが限られているレポートでの利用を推奨します。

フィルター追加 ユーザー 追加

条件1

操作 選択なし 操作一覧

Operation [対象とする] AND OR [UserLoginFailed] [除外する] AND OR 複数指定する場合、改行区切りで入力します。

プレビュー(レポート) プロパティ ファイル出力 メール通知 詳細設定 高度な設定

OK キャンセル

現在のレポート定義でどのようなレポート出力が出来るか確認する為に「プレビュー (レポート)」をクリック。



プレビュー

2020/07/01 - 2020/07/31

1 検索条件: 1件

時刻	ユーザー	グループ	SessionID	詳細
1 2020/07/28 14:09:12	PC-2015-09-254.amiya.co.jpSecurity	PC-2015-09-254.amiya.co.jp	1102	9-1-5-21-1908713992-750736408-2091147243-761010mish

レポート定義に問題が無く、該当のログがDBに保存されている場合、レポート結果を確認する事が可能です。

<ご不明な点があればこちらまでお問い合わせ下さい>

MAIL : bv-support@amiya.co.jp

TEL : 03-6822-9910